

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, CA 90010-1137

Justin F. Marquez, SBN 262417
justin@wilshirelawfirm.com
Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Robert J. Dart, SBN 264060
rdart@wilshirelawfirm.com
April Yang, SBN 330951
april@wilshirelawfirm.com
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

*Attorneys for Plaintiff LAVARIOUS GARDINER
and Proposed Class Counsel*

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

LAVARIOUS GARDINER, individually
and on behalf of all others similarly situated,

Plaintiff,

v.

WALMART INC., a Delaware corporation;
DOES 1 to 10, inclusive,

Defendants.

CASE NO.: 4:20-cv-04618-JSW

CLASS ACTION

AMENDED COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Lavarious Gardiner, individually, and on behalf of all others similarly situated, brings this action based upon his personal knowledge as to himself and his own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigation of his attorneys.

NATURE OF THE ACTION

1. Defendant Walmart, Inc. (“Walmart”) is a retailer selling goods at its stores and online via its website. Hundreds of millions of customers shop at Walmart every week at its physical store locations and on its website. Those customers reasonably expect the most stringent level of protection for their personally identifiable information (“PII”) when entrusting their

1 highly sensitive information – including home addresses and credit card numbers – to Walmart,
2 as is required to complete purchases online and/or create a customer account on Walmart’s
3 website. What Walmart customers did not and do not expect is that their personal and sensitive
4 information, including access to their credit card and financial accounts, would be harvested by
5 unauthorized individuals from Walmart’s website and sold on the dark web. And yet that is
6 precisely what has happened, with the account information and data of thousands, if not millions,
7 of Walmart customers currently available for sale on the dark web.

8 2. Plaintiff, individually, and on behalf of those similarly situated persons (hereafter,
9 “Class Members”), brings this class action to secure redress against Defendants for their reckless
10 and negligent violation of customer privacy rights. Plaintiff and Class Members are individuals
11 who were customers of Walmart during at least the four-year period prior to the date of the filing
12 of this Complaint to the present.

13 3. Plaintiff and Class Members suffered significant injuries and damages. The
14 security breach compromised the full names, addresses, financial account information, credit card
15 information, and other PII of Walmart’s customers.

16 4. As a result of Defendants’ wrongful actions and inactions, unauthorized
17 individuals gained access to and harvested Plaintiff’s and Class Members’ PII from Walmart’s
18 website. Walmart’s website’s vulnerabilities led to direct breaches of Walmart’s internal data
19 systems. Plaintiff and Class Members have been forced to take remedial steps to protect
20 themselves from future loss and injury. Indeed, all Class Members currently remain at a very
21 high risk of identity theft and/or credit card fraud, and prophylactic measures, such as the purchase
22 of credit monitoring services and software, are reasonable and necessary to prevent and/or
23 mitigate future loss.

24 5. As a result of Defendants’ wrongful actions and inactions, highly sensitive
25 customer information was stolen. Many customers of Walmart have had their PII compromised,
26 their privacy rights violated, have been exposed to a critical and continuing risk of fraud and
27 identify theft, and have otherwise suffered damages.

6. Though Plaintiff's transaction occurred prior to that date, there is evidence that the breach occurred after or has continued through January 1, 2020. PII from Walmart customers available for purchase on the dark web includes credit card data from credit cards which, due to their expiration dates, could not have been issued prior to January 1, 2020. As there is evidence indicating a single, continuous, and unaddressed data breach that has compromised Walmart customers' data, it appears that Plaintiff's data, which he first entrusted to Walmart in 2016, was "stored" in Walmart's systems or records and then later exposed in a data breach occurring after or continuing through January 1, 2020.

THE PARTIES

8. Plaintiff Lavarious Gardiner is a California citizen residing in San Francisco, California. Plaintiff is a customer who entrusted his PII to Walmart – a necessary step in the process of making online purchases and/or creating a customer account from Walmart’s website. Plaintiff is informed and believes that his PII was accessed by hackers as a direct result of a breach in Walmart’s cybersecurity environment and internal data systems. Plaintiff made a purchase from Walmart’s website in 2016, at which time he entrusted Defendants with his PII and payment information. Plaintiff does not recall any requirement, during the checkout process on Walmart’s website, that he accept or assent to Walmart’s Terms of Use. At some point thereafter, Plaintiff’s stored customer data, containing his PII and financial information, was compromised and all of the data associated with his Walmart purchases is currently being sold on the dark web. Consequently, as a necessary and reasonable measure to protect himself from further injury,

1 Plaintiff purchased a credit and personal identity monitoring service to alert him to any potential
2 misappropriation of his data and to combat further risk of identity theft. At a minimum, therefore,
3 Plaintiff has suffered compensable damages because his data, which has a monetary value, is
4 being sold on the dark web against his will and he has been forced to purchase a credit monitoring
5 service out-of-pocket – a reasonable and necessary prophylactic step to prevent and/or mitigate
6 future loss. Exposure of Plaintiff’s PII as a result of the Walmart data breach has placed him at
7 an imminent, immediate, and continuing risk of further harm for which he will need to expend
8 time and labor to combat and prevent.

9 9. Defendant Walmart Inc. is a Delaware corporation with its principal place of
10 business located in Bentonville, Arkansas.

11 10. Plaintiff is unaware of the true names, identities, and capacities of the defendants
12 sued herein as DOES 1 to 10. Plaintiff will seek leave to amend this complaint to allege the true
13 names and capacities of DOES 1 to 10 if and when ascertained. Plaintiff alleges, upon
14 information and belief, that each of the defendants sued herein as a DOE is legally responsible in
15 some manner for the events and happenings alleged herein, and, as set forth below, that each of
16 the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiff and
17 Class Members.

18 11. As used herein, “Defendants” shall refer to Walmart Inc. and Does 1 to 10,
19 collectively.

20 **JURISDICTION AND VENUE**

21 12. This Court has subject matter jurisdiction over the state law claims asserted herein
22 pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class
23 Members are citizens of a State different from the Defendant; there are more than 100 putative
24 class members; and the amount in controversy exceeds \$5,000,000.

25 13. The Court also has personal jurisdiction over the parties because, on information
26 and belief, Defendants conduct a major part of their domestic operations with regular and
27 continuous business activity in California, through a large number of stores and with an
28 advertising budget not exceeded in other jurisdictions throughout the United States. Plaintiff’s

1 and the Class Members' claims arise out of Defendants' business activities in California because
 2 Plaintiff's and the Class Members purchased items from the Walmart's website and/or created
 3 Walmart customer accounts in and while residing in California and have suffered their injuries in
 4 and while residing in California.

5 14. Venue is appropriate in this District because, among other things: (a) Defendants
 6 directed their activities at residents in this District; and (b) many of the acts and omissions that
 7 give rise to this Action took place in this judicial District.

8 **FACTUAL ALLEGATIONS**

9 ***A. Walmart's Data Breach***

10 15. Walmart is a major American retailer, operating numerous stores and selling goods
 11 via its website. Customers patronizing Walmart's online store must provide Walmart with PII in
 12 order to make purchases and/or create customer accounts, including full names, mailing and
 13 billing addresses, phone numbers, email addresses, and payment information, usually in the form
 14 of credit or debit card information. Walmart has been the target of at least one successful hack in
 15 recent years. Hackers have obtained access to Walmart customer data and/or accounts by hacking
 16 Walmart's website and Walmart's customers' computers by exploiting vulnerabilities on
 17 Walmart's website and subsequently selling the stolen customer information on the dark web.

18 16. That Walmart has been successfully hacked is illustrated by the fact that the dark
 19 web is replete with stolen Walmart customer data and customer accounts for sale. Over two
 20 million customer data and/or accounts are available for sale on websites such as
 21 [http://wwhclubl4tefzrzf.onion/index.php?threads/skupaju-gifty-amazon-carters-walmart-old-](http://wwhclubl4tefzrzf.onion/index.php?threads/skupaju-gifty-amazon-carters-walmart-old-navy-pod-vysokij.58790/page-12/)
 22 navy-pod-vysokij.58790/page-12/, and <http://blackpasqk3nqfuc.onion/>. Many similar
 23 "marketplaces" exist.

24 17. These sale listings on dark web marketplaces contain only enough PII to prove to
 25 potential buyers that the sellers really do possess all the information associated with each data set
 26 or account. In 2019, Plaintiff learned that his PII was put up for sale in one such marketplace:
 27 <http://blackpasqk3nqfuc.onion/>. Included in the seller's listing containing Plaintiff's PII were
 28

1 Plaintiff's name, home address, phone number, and the last four digits and expiration dates of two
2 of his debit cards.

3 18. Plaintiff confirmed through extensive online searches that the names, phone
4 numbers, and addresses for many – if not all – of the other individuals whose information is being
5 sold on these marketplaces are correct and verifiable. The verifiability of these forms of PII in
6 the sale listings indicates the substantial likelihood that the payment information advertised in the
7 listings, including last four digits and expiration dates of credit and debit cards, is also legitimate
8 and within the sellers' possession. In fact, sellers in dark web marketplaces purposely refrain
9 from posting all of the data they possess for a customer, otherwise they would have nothing left
10 to sell. Instead, sellers list just enough customer PII to validate that they do indeed possess all of
11 the information they claim to possess – including full credit and debit card numbers, and PIN and
12 CVV codes associated with those payment cards. No purchaser would purchase the information
13 if it did not include PIN and CVV information, so it must be concluded that this information is
14 included in the items for sale. Then, once a buyer purchases the data set or account information
15 from the seller, the seller then turns over the remainder of the PII and payment information that
16 would allow the buyer to commit financial fraud and identity theft crimes. Thus, the harm to the
17 customer is committed at the time when the customer's PII is improperly accessed and stolen, and
18 then when the PII is first posted on the dark web for sale, as there is a robust market for such
19 stolen personal and financial information. At that point, any subsequent harm to a customer
20 whose PII has been sold on the dark web is more of an eventuality than a mere possibility.

21 19. Despite the fact that the PIN or CVV numbers associated with Plaintiff's payment
22 cards were not listed in the seller's posting on the dark web, Plaintiff undoubtedly entrusted
23 Defendants with this information in the course of completing his online purchase, otherwise
24 Walmart would not have been able to charge his debit card and finalize the transaction. The seller
25 of Plaintiff's PII possesses Plaintiff's PIN or CVV numbers associated with his payment cards
26 and was only withholding publication of that information until a buyer made an acceptable offer
27 for the PII.
28

20. Cybercriminals have been selling stolen Walmart customer data and/or accounts on dark web marketplaces from January 24, 2020 to May 17, 2020, at the very least. Walmart customer data and/or accounts being sold by these websites during this time period include data and accounts dated in 2020, along with data and accounts that date back as far back as March 28, 2019.

21. Many of the “last order dates” contained in records of stolen customer information that have been found are from 2020, indicating that the data came from a breach that occurred in 2020. “Last order dates” are the dates of a customer’s last purchase on Defendants’ website before the PII was stolen. Furthermore, certain information contained within some of these stolen data sets and/or accounts, such as credit card information, could not have been issued prior to January 1, 2020 based upon their expiration date.

22. Moreover, Plaintiff retains in his possession communications with the hackers in which they state that the data sets and/or accounts they are selling are real data sets and/or accounts that belong to Walmart customers.

23. Further, the fact that Walmart has been hacked is illustrative of the fact that its systems are quite vulnerable to unauthorized access, misuse of information, and disruption. A scan of Walmart’s domains using Open Web Application Security Project Zed Attack Proxy (“OWASP ZAP”), which is widely used in the cybersecurity community to scan websites for documented vulnerabilities, resulted in the exposure of six major vulnerabilities.

24. These vulnerabilities include:

- Seven instances of private IP addresses being disclosed in the public website code. While this is not a direct attack vector, it may contribute to an attack on Walmart’s systems.
- 44 instances of password autocomplete enabled. This could potentially contribute to a hacker’s breach of a user’s data set and/or account. If a script or malware is running on the customer’s computer, the script or malware can extract the password from the browser.
- 112,118 instances of the Cookie No HttpOnlyFlag being set, which means that cookies

can be accessed by scripts or malware on the client machine. This can be used to conduct session hijacking attacks. If the customer has malware on his or her computer, that malware can manipulate and access cookie data.

- 8,615 instances of cross-site scripting (“XSS”) protection not enabled. This is a very serious issue, which means that the site could be vulnerable to the common cross site scripting attack. In such an attack, the hacker injects client-side script into web pages which are viewed by other users, typically targeting areas in which there is a high level of user interaction. When the user interacts with those areas, the website executes the attacker’s script rather than the intended website functionality. This would enable the hacker to steal information from the customers.
- 100,061 instances of Cross Domain JavaScript source file inclusion. This would also allow a hacker to perform cross site scripting, by inserting malicious JavaScript.
- 93,060 instances of a cookie without the secure flag being set. This is similar to the No HttpOnlyFlag being set, in that it enables cookies to be accessed through unencrypted connections.

25. An OWASP ZAP scan of <http://grocery.walmart.com> and the IP address for Walmart photos revealed similar vulnerabilities on those websites.

26. Scans using other highly respected vulnerability scanners resulted in affirmation of the aforementioned vulnerabilities, and the finding of additional vulnerabilities which hackers can take advantage of to obtain protected files from a website. For example, a scan of less than 2% of the Walmart website using the Vega vulnerability scanner uncovered 228 high ranked vulnerabilities. These vulnerabilities include the integer overflow vulnerability. Within the integer overflow vulnerability were exposed numbers, of which 224 appeared to be in the format of social security numbers, and multiple numbers that appeared to be in the format of credit card numbers. Vega also found 7 instances where local paths were revealed, which can allow hackers to obtain sensitive information about the server environment.

27. Plaintiff also conducted a scan of the website using the Nessus tool. Government agencies that use the Nessus tool to scan websites include the IRS, Argonne National Lab,

1 Defense Information Systems Agency, Department of Defense, U.S. Navy, and others. Plaintiff
 2 utilized the Nessus PCI scan. PCI stands for Payment Card Industry, and the Nessus PCI scan
 3 tests the website against the PCI DSS standards, which organizations must follow if they accept
 4 payment cards from major credit card brands. A company that is not PCI compliant can be fined
 5 and, in some cases, their payment card privileges can be revoked. Defendants are not PCI
 6 compliant. The scan showed 20 PCI vulnerabilities, each ranked as high, and identified the
 7 following severe issues, each of which would be considered to be an “automatic failure,”
 8 according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1):

- 9 • Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- 10 • Unsupported operating systems;
- 11 • Internet reachable database servers;
- 12 • Presence of built-in or default accounts;
- 13 • Unrestricted DNS Zone transfers;
- 14 • Unvalidated parameters leading to SQL injection attacks;
- 15 • XSS flaws;
- 16 • Directory traversal vulnerabilities;
- 17 • HTTP response splitting/header injection;
- 18 • Detection of backdoor applications (malware, trojan horses, rootkits, backdoors);
- 19 • Use of older, insecure SSL/TLS versions;
- 20 • Use of anonymous key exchange protocols (such as anonymous Diffie-Hellman in
- 21 SSL/TLS); and
- 22 • Scan Interference.

23 28. The Nessus PCI scan also located three problems with Walmart.com’s SSL/TLS
 24 certificates. SSL/TLS stands for Secure Sockets Layer/Transport Layer Security and is how
 25 websites encrypt data transmissions. SSL/TLS utilizes digital certificates to encrypt data.
 26 Security flaws in SSL/TLS certificates make all transmissions vulnerable, including transmissions
 27 of credit card information and account details.
 28

29. The Nessus PCI scan identified the following problems with Walmart.com's SSL/TLS certificates: SSL certificate cannot be trusted, SSL certificate with wrong hostname, and SSL self-signed certificate. Each of these problems means that data transmissions on the website are vulnerable.

30. The Nessus PCI scan also revealed that Defendants are using an outdated protocol, TLS Version 1.1, which is technology that was replaced 12 years ago and has known weaknesses.

31. The net result of these security flaws allows hackers to access and exfiltrate a large amount of Walmart's customer data in a single, inclusive data breach. Due to the aforementioned vulnerabilities in how customer information is stored on Walmart.com, information obtained in such a breach could potentially include customer information that had been entered into Walmart's website prior to the actual date of the breach.

C. California Recognizes the Importance of PII

32. *California Civil Code* § 1798.81.5(a)(1) states that: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

D. Stolen Information Is Valuable to Hackers and Thieves

33. It is widely recognized, and the subject of many media reports, that PII is a highly coveted commodity and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation regarding data breached, frequent public announcements of data breaches, and having fallen victim to hacks in the past, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class Members. *See* <http://www.wired.com/2009/10/walmart-hack/>.

34. Legitimate organizations and members of the criminal underground alike recognize the value of PII. Otherwise, they would not aggressively seek and pay for it. As previously seen in one of the world's largest data breaches, hackers compromised the card holder data of 40 million customers of Target, another "big box" store very comparable to Walmart. *See*

1 “Target: 40 million credit cards compromised,” CNN Money, Dec. 19, 2013, *available at*
 2 [http://money.cnn.com/2013/12/18/news/companies](http://money.cnn.com/2013/12/18/news/companies/target-credit-card/)
 3 [/target-credit-card/](http://money.cnn.com/2013/12/18/news/companies/target-credit-card/), attached hereto as **Exhibit A**. In contrast, DataCoup provides just one
 4 example of a legitimate business that pays users for personal information. *See*
 5 <http://money.com/money/3001361/datacoup-facebook-personal-data-privacy/>, attached hereto as
 6 **Exhibit B**.

7 35. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of
 8 crimes, including credit card fraud, phone or utilities fraud, and bank/financial fraud. PII that is
 9 stolen from the point of sale are known as “dumps.” *See* Krebs on Security April 16, 2016, Blog
 10 Post, *available at* <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/>,
 11 attached hereto as **Exhibit C**. PII can be used to clone a debit or credit card. *Id.*

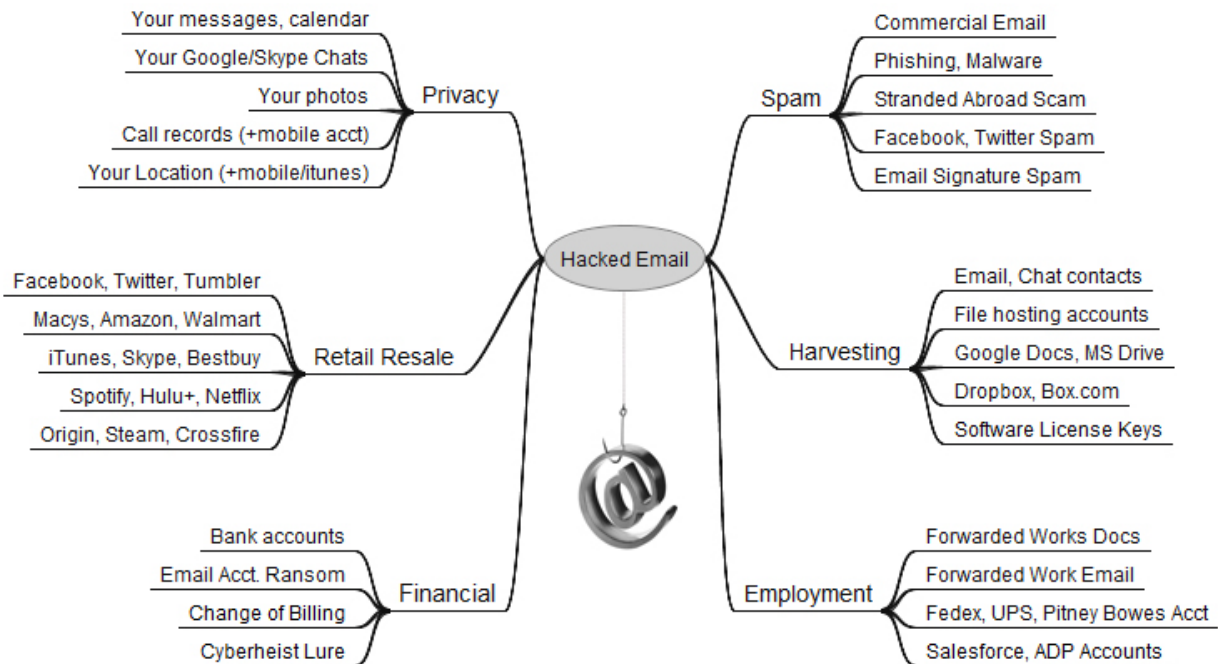
12 36. Once someone buys PII, it is then used to gain access to different areas of the
 13 victim’s digital life, including bank accounts, social media, and credit card details. During that
 14 process, other sensitive data may be harvested from the victim’s accounts, as well as from those
 15 belonging to their family members, friends, and colleagues.

16 37. In addition to PII, a hacked email account can be very valuable to cybercriminals.
 17 Since most online accounts require an email address not only as a username, but also as a way to
 18 verify accounts and reset passwords, a hacked email account could open up a number of other
 19 accounts to an attacker.¹

20 38. As shown below, a hacked email account can be used by an identity thief to link
 21 to many other sources of information, including any purchase or account information found in the
 22 hacked email account.²

26 ¹ Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015),
 27 [https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-](https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data)
 28 [value-of-your-personal-data](https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data).

² Brian Krebs, The Value of a Hacked Email Account, Krebs on Security (June 13, 2013, 3:14 PM), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>.



39. Hacked information can also enable thieves to obtain other personal information through “phishing.” According to the Report on Phishing available on the United States, Department of Justice’s website: “AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers, and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.”³

40. In addition to transactions involving PII on the dark web, transactions involving PII also occur legally on “white” markets, which provides further corroboration that PII has real, provable, and monetary value. This is evidenced by the fact that tech giants, such as Facebook, have spent billions of dollars acquiring social media websites and platforms, transactions in which one of the primary (if not the most valuable) assets sought and acquired is user or customer PII.

41. Finally, there are now startup companies designing platforms on which users can take control of and monetize their own personal data. One such company, UBDI, was founded in 2018 and its mission is to create a “Universal Basic Data Income” stream. UBDI’s platform

³ https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

allows users to link their accounts from other websites and applications, such as Spotify, Twitter, and Apple Health – which can contain both user PII and PHI – for “opportunities to earn in data studies” by essentially selling UBDI access to their personal data. *See* <https://www.ubdi.com/>. The value of PII can be evidenced using market-based pricing data from both dark and white web marketplaces. This well-established and peer-reviewed “market approach” is premised on the idea that the fair market value of an item, whether tangible or intangible, is evidenced by the amount that buyers and sellers would negotiate for the item in a market transaction. Because it is possible to assign a monetary value to PII using a market approach, it is of no consequence whether or not Plaintiff has ever intended, or intends in the future, to sell his own PII in either a legal or illegal market. Based on these tested and methodologically sound statistical approaches, it is clear that PII is arising, in this digital age, as an increasingly commodified and exchanged intangible asset with an undeniable, intrinsic value – a value of which victims of a data breach are wrongfully deprived.

E. The Data Breach Has Resulted and Will Result in Identity Theft and Identity Fraud

42. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiff and Class Members.

43. The ramifications of Defendants’ failure to keep Plaintiff’s and Class Members’ PII secure is severe. According to Javelin Strategy and Research, “one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year.” “Someone Became an Identity Theft Victim Every 2 Seconds Last Year,” Fox Business, Feb. 5, 2014 *available at* <http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html> attached hereto as **Exhibit D**.

44. In the case of a data breach, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”) found that “among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.” *See* “Victims of Identity Theft,” U.S. Department of Justice, Dec 2013, *available at*

1 <https://www.bjs.gov/content/pub/pdf/vit12.pdf> attached hereto as **Exhibit E**. In fact, the BJS
2 reported, “resolving the problems caused by identity theft [could] take more than a year for some
3 victims.” *Id.* at 11.

4 45. A person whose PII has been obtained and compromised may not know or
5 experience the full extent of identity theft or fraud for years. It may take some time for the victim
6 to become aware of the theft or fraud. In addition, a victim may not become aware of fraudulent
7 charges when they are nominal because typical fraud-prevention algorithms fail to capture such
8 charges. Those charges may be repeated, over and over again, on a victim’s account without
9 notice for years.

10 ***F. Annual Monetary Losses from Identity Theft are in the Billions of Dollars***

11 46. According to the BJS, an estimated 17.6 million people were victims of one or
12 more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit
13 card accounts were the most common types of misused information. *Id.*

14 47. Javelin Strategy and Research reports that losses from identity theft reached \$21
15 billion in 2013. *See* 2013 Identity Fraud Report, attached hereto as **Exhibit F**. There may be a
16 “dormant period” between when harm occurs and when it is discovered, and also between when
17 PII is stolen and when it is used. According to the U.S. Government Accountability Office
18 (“GAO”), which conducted a study regarding data breaches:

19 [L]aw enforcement officials told us that in some cases, stolen data may be held for
20 up to a year or more before being used to commit identity theft. Further, once
21 stolen data have been sold or posted on the Web, fraudulent use of that information
22 may continue for years. As a result, studies that attempt to measure the harm
23 resulting from data breaches cannot necessarily rule out all future harm.

24 See GAO, Report to Congressional Requesters, at 33 (June 2007), *available at*
25 <http://www.gao.gov/new.items/d07737.pdf>, attached hereto as **Exhibit G**.

26 48. As a result of the data breach, Plaintiff and Class Members now face years of
27 continuous monitoring and surveillance of their financial and personal records, and intrusion on
28 their privacy rights. Plaintiff and Class Members are also subject to a higher risk of phishing and

pharming whereby hackers exploit information they already obtained in an effort to procure even more PII. Plaintiff and Class Members are presently incurring and will continue to incur such damages, in addition to any fraudulent credit and debit card charges, and the resulting loss of access to their funds or lines of credit when those accounts must be frozen or modified whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiff and Class Members now run the risk of unauthorized individuals opening credit card or bank account, taking out loans or mortgages, and engaging in other fraudulent conduct using their identities.

G. Plaintiff and Class Members Suffered Damages

49. The exposure of Plaintiff's and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by a common law duty of care, which is established by federal information security standards. The data breach was a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, as also required by federal standards.

50. Plaintiff's and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendants. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and financial fraud, requiring them to expend time and effort to mitigate the actual and potential impact of the data breach on their lives by, among other things, placing "freezes" on and setting up "alerts" with credit reporting agencies for their accounts, contacting and following up with their financial institutions, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. Plaintiff and Class Members have also incurred out-of-pocket expenses including, but not limited to, for credit monitoring and identity theft protection subscription

1 services, postage costs, and hiring attorneys, accountants, and other specialists to assist with
2 recovery and mitigation efforts.

3 51. Although many large corporations that suffer data breaches now commonly offer
4 their affected customers one free year of credit monitoring services, there are notable differences
5 between these free services and “compensated” services (those that customers must pay for out-
6 of-pocket). Compensated services provide additional, and downright necessary, benefits that are
7 usually not included with the free services offered by these companies. These added benefits
8 include monitoring for stolen funds and personal expenses, legal insurance protections, enhanced
9 financial account monitoring, and access to resolution/restoration specialist services. On June 9,
10 2020, Plaintiff was made to purchase one such compensated credit monitoring service, Norton
11 LifeLock, which renews annually, and which Plaintiff expects to continue paying for in perpetuity
12 as a result of this data breach.

13 52. The website for Norton LifeLock, a popular and reputable data protection services
14 provider, recommends that, even with the purchase of monitoring services, victims of a data
15 breach should still “stay alert” and “monitor [their] accounts closely.” Other major companies,
16 including U.S. News and Experian, have issued similar guidance to continuously review credit
17 reports, mail, and billing statements for signs of fraud after suffering a data breach.. All of these
18 monitoring activities cost not only money, but time and effort. This time and effort may not
19 appear facially to be a significant day-to-day expense but, in the aggregate over the course of
20 years, will cost the victims of data breaches hours of their free time and much turmoil.

21 53. Breach-related damages in the form of lost time can reasonably be quantified
22 monetarily and calculated as a function of hours spent times a labor rate. One reasonable method
23 of assigning a monetary value to the time spent by victims to respond to and mitigate the
24 consequences of a data breach is to determine the rate these victims would have to pay a specialist
25 – such as an administrative assistant, accountant, bookkeeper, or auditor – to perform the
26 monitoring activities that they must otherwise conduct themselves. Plaintiff and Class Members
27 have already or will need to spend hours of their time monitoring their financial and credit
28 accounts for indicia of fraud now that their PII has been leaked, not knowing who has now had

1 access to their PII or what those actors may one day do with it. This time has been spent by
2 Plaintiff and the Class Members, just as they have spent their money mitigating the damage from
3 Defendants' data breach, as this lost time has real and calculable monetary value. And just as
4 Plaintiff's and Class Members' out-of-pocket expenditures were reasonable and necessary to
5 protect themselves from further damage resulting from the data breach, so too was Plaintiff's and
6 Class Members' expenditure of time and labor on such mitigation efforts.

7 54. In *Corona v. Sony Pictures Entertainment Inc.*, the Court ruled that credit
8 monitoring may be compensable in a data breach action "where evidence shows that the need for
9 future monitoring is a reasonably certain consequence of the defendant's breach of duty, and that
10 the monitoring is reasonable and necessary." *Corona v. Sony Pictures Ent., Inc.*, 2015 WL
11 3916744, at *4 (C.D. Cal. June 15, 2015). To determine the reasonableness and necessity of such
12 credit monitoring services, the Court considered a five-factor test laid out in *Potter v. Firestone*
13 *Tire & Rubber Co.* As adapted to the data breach context, those factors are: (1) the significance
14 and extent of the compromise to Plaintiffs' PII; (2) the sensitivity of the compromised
15 information; (3) the relative increase in the risk of identity theft when compared to (a) Plaintiffs'
16 chances of identity theft had the data breach not occurred, and (b) the chances of the public at
17 large being subject to identity theft; (4) the seriousness of the consequences resulting from identity
18 theft; and (5) the objective value of early detection. *Potter v. Firestone Tire & Rubber Co.*, 6
19 Cal.4th 965, 1008 (1993).

20 55. Upon review of the allegations, the *Corona* Court found that Plaintiffs' factual
21 allegations supported the reasonableness and necessity of Plaintiffs' credit monitoring. First,
22 Plaintiffs allege that Sony's data breach resulted in the public disclosure of its employees' most
23 sensitive, non-public PII, including names, home and email addresses, and bank account
24 information. *Corona*, 2015 WL 3916744 at *4. These records were posted on file-sharing
25 websites and traded on torrent networks. *Id.* As to the risk of identity theft, the Court found it
26 reasonable to infer that the data breach and resulting publication of Plaintiffs' PII drastically
27 increased their risk of identity theft, relative to both the time period before the breach, as well as
28 to the risk born by the general public. *Id.* The Court determined that it is commonly known that

1 the consequences resulting from identity theft can be both serious and long-lasting. *Id.* Lastly,
2 the Court found allegations that some plaintiffs had already received notification of attempted
3 identity theft highlighted the value of early detection. *Id.*

4 56. Here, Plaintiff's injuries – the exposure of his name, home address, phone number,
5 and payment information on dark websites – are remarkably similar to those suffered by the
6 plaintiffs in *Corona*. This publication of Plaintiff's PII has certainly drastically increased his risk
7 of identity theft, the consequences of which would be serious and long-lasting. The sale of
8 Plaintiff's PII on the dark web can reasonably be characterized as an attempted identity theft and
9 Plaintiff's discovery of his most personal information on the dark web marketplace has inarguably
10 highlighted the value of early detection of future fraud and misuse of his PII. Plaintiff's purchase
11 of credit monitoring to mitigate damages resulting from Defendants' data breach was both
12 reasonable and necessary and, therefore, compensable.

13 57. Defendants' wrongful actions and inactions directly and proximately caused the
14 theft and dissemination of Plaintiff's and Class Members' PII into the public domain, causing
15 them to suffer, and continue to suffer, economic damages and other actual harm for which they
16 are entitled to compensation, including:

- 17 a. The improper disclosure, compromise, and theft of their PII;
- 18 b. The imminent and certainly impending injury flowing from potential fraud and
19 identity theft posed by the unauthorized access and misappropriation of their PII by
20 hackers, namely through the sale of Plaintiff's and Class Members' information on
21 the dark web;
- 22 c. The lack of any notification of the data breach;
- 23 d. Ascertainable losses in the form of out-of-pocket expenses and the value of their
24 time reasonably incurred to remedy or mitigate the effects of the data breach;
- 25 e. Ascertainable losses in the form of deprivation of the value of their PII, for which
26 there are well-established dark and white web markets;
- 27
- 28

f. Harms that cannot be quantified or remedied by monetary damages, such as lowered credit scores and identity theft, that can cause long-term and continuing socioeconomic consequences; and

g. Overpayments to Defendants for the goods bought from Defendant, as Plaintiff and Class Members relied on the reasonable assumption that some proportion of the revenue earned by Defendants from the transactions with Class Members would be allocated to the implementation of reasonable and adequate data security measures that would protect their PII. Had Plaintiff and Class Members known before entering into these transactions that Defendants would not protect their PII from unauthorized access and use, Plaintiff and Class Members would not have paid the agreed-upon amounts for Defendants' goods.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this action on his own behalf and on behalf of a class of individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiff intends to seek certification of a class defined as follows:

All persons residing in the State of California who made online purchases from Walmart's website at any time from four years prior to the date of the filing of the Complaint to the date on which notice was sent to the class (the "Class").

59. Excluded from the Class are: (a) Defendants, including any entity in which any of the Defendants has a controlling interest, is a parent or a subsidiary of, or which is controlled by any of the Defendants; (b) the officers, directors, and legal representatives of Defendants; and (c) the judge and the court personnel in this case as well as any members of their immediate families. Plaintiff reserves the right to amend the definition of the Class if discovery, further investigation and/or rulings by the Court dictate that it should be modified.

60. *Numerosity.* The members of the Class are so numerous that the joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, given the number of Walmart customers in California, it stands to reason that the

number of Class Members is at least in the thousands. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as customer account information.

61. *Commonality and Predominance.* This action involves questions of law and fact common to all Class Members that predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants owed a duty of care to Plaintiff and Class Members with respect to the security of their PII;
- b. What security measures must be implemented by Defendants to comply with their duty of care;
- c. Whether Defendants met the duty of care owed to Plaintiff and the Class Members with respect to the security of the PII;
- d. The nature of the relief, including equitable relief, to which Plaintiff and Class Members are entitled; and
- e. Whether Plaintiff and Class Members are entitled to damages, civil penalties and/or injunctive relief.

62. *Typicality.* Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of each of the other Class Members, was exposed and/or improperly disclosed by Defendants.

63. *Adequacy of Representation.* Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intends to prosecute this action vigorously. Plaintiff and Class Members have a unified and non-conflicting interest in pursuing the same claims and obtaining the same relief. Therefore, all Class Members will be fairly and adequately represented by Plaintiff and his counsel.

64. *Superiority of Class Action.* A class action is superior to other available methods for the fair and efficient adjudication of the claims alleged in this action. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially

1 conflicting adjudications of the asserted claims. There will be no difficulty in the management
 2 of this action as a class action, and the disposition of the claims of the Class Members in a single
 3 action will provide substantial benefits to all parties and to the Court. Damages for any individual
 4 Class Member are likely insufficient to justify the cost of individual litigation so that, in the
 5 absence of class treatment, Defendants' violations of law inflicting substantial damages in the
 6 aggregate would go un-remedied.

7 65. Class certification is also appropriate because Defendants have acted or refused to
 8 act on grounds generally applicable to the Class Members, such that final injunctive relief or
 9 corresponding declaratory relief is appropriate as to the Class as a whole.

10 **FIRST CAUSE OF ACTION**

11 (Violation of the California Consumer Privacy Act ("CCPA"), Civ. Code § 1798.150 *et seq.*)

12 66. Plaintiff repeats and incorporates by reference each and every allegation contained
 13 in paragraphs 1 through 65, inclusive of this Complaint as if set forth fully herein.

14 67. Under Civ. Code § 1798.150(a)(1),

15 "Any consumer whose nonencrypted and nonredacted personal
 16 information, as defined in subparagraph (A) of paragraph (1) of subdivision
 17 (d) of Section 1798.81.5, is subject to an unauthorized access and
 18 exfiltration, theft, or disclosure as a result of the business's violation of the
 19 duty to implement and maintain reasonable security procedures and
 20 practices appropriate to the nature of the information to protect the personal
 21 information may institute a civil action for any of the following:

22 (A) To recover damages in an amount not less than one
 23 hundred dollars (\$100) and not greater than seven hundred
 24 and fifty (\$750) per consumer per incident or actual
 25 damages, whichever is greater.

26 (B) Injunctive or declaratory relief.

27 (C) Any other relief the court deems proper."
 28

1 68. Plaintiff and the Class Members provided to Defendants its nonencrypted and
2 nonredacted personal information as defined in § 1798.81.5 in the form of their PII.

3 69. Plaintiff and the Class Members' PII was subject to an unauthorized access and
4 exfiltration when it was stolen by hackers and posted on the dark web for sale.

5 70. It is probable that this unauthorized access and exfiltration of Plaintiff and Class
6 Member's PII occurred as the result of a single, inclusive data breach of Walmart.com.

7 71. This unauthorized access and exfiltration occurred after January 1, 2020, because
8 certain stolen PII that was discovered to be a part of the same data breach that Plaintiff's PII was
9 a part of could not have been issued prior to January 1, 2020. Many of the "last order dates" of
10 stolen customer data that have been found on the dark web are from 2020, further supporting that
11 said data came from a breach that occurred in 2020. In addition, the stolen data includes credit
12 cards with expiration dates occurring sufficiently in advance such that the cards could not have
13 been issued before January 1, 2020.

14 72. These credit and debit card expiration dates provide sound evidence that those
15 customer accounts and data must have been stolen from Walmart's website after January 2020.
16 Some of the credit and debit card information listed for sale have expiration dates in 2024 and
17 2025. Credit cards are generally configured to expire after three years. *See*
18 <https://wallethub.com/edu/cc/credit-cards-expiration-date/25566/>. For example, Capital One
19 specifically states that its credit cards expire after three to five years. *See*
20 [https://www.capitalone.com/learn-grow/money-management/credit-card-expiration-and-](https://www.capitalone.com/learn-grow/money-management/credit-card-expiration-and-replacement/)
21 [replacement/](https://www.capitalone.com/learn-grow/money-management/credit-card-expiration-and-replacement/). American Express Corporate cards expire after four years. *See*
22 [https://business.americanexpress.com/ru/en/frequently-asked-questions/icc-corporate-](https://business.americanexpress.com/ru/en/frequently-asked-questions/icc-corporate-cardprogram/faq-1/)
23 [cardprogram/faq-1/](https://business.americanexpress.com/ru/en/frequently-asked-questions/icc-corporate-cardprogram/faq-1/). EDD debit cards in California expire after three years. *See*
24 https://edd.ca.gov/about_edd/The_EDD_Debit_Card.htm/. Given these examples from major
25 card issuers, there is a high probability that many of the sale listings containing Walmart
26 customers' payment information are for credit and debit cards that were issued after January 2020.
27 This indicates that the breach in Defendants' cybersecurity environment must have either first
28 occurred after or continued through January 2020.

73. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff and the Class Members' PII was a result of Walmart's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. A scan of Walmart's domains using OWASP ZAP resulted in the exposure of six major vulnerabilities, which include:

- Private IP addresses being disclosed in the public website code.
- 44 instances of password autocomplete enabled.
- The cookie No HttpOnlyFlag being set, which means that cookies can be accessed by scripts or malware on the client machine.
- 8,615 instances of XSS protection not enabled.
- 100,061 instances of Cross Domain JavaScript source file inclusion.
- 93,060 instances of a cookie without the secure flag being set.

74. An OWASP ZAP scan of <http://grocery.walmart.com> and the IP address for Walmart photos revealed similar vulnerabilities on those websites.

75. After scanning less than 2% of the Walmart website using the Vega vulnerability scanner, 228 high ranking vulnerabilities materialized. Within the integer overflow vulnerability were exposed numbers, of which 224 appeared to be in the format of social security numbers, and multiple numbers that appeared to be in the format of credit card numbers. Vega also found 7 instances where local paths were revealed, which can allow hackers to obtain sensitive information about the server environment.

76. A scan using the Nessus PCI tool scan revealed 20 PCI vulnerabilities, each ranked as high, and identified the following severe issues, each of which would be considered to be an "automatic failure" according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1):

- Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- Unsupported operating systems;
- Internet reachable database servers;
- Presence of built-in or default accounts;

- Unrestricted DNS Zone transfers;
- Unvalidated parameters leading to SQL injection attacks;
- Cross-Site Scripting (XSS) flaws;
- Directory traversal vulnerabilities;
- HTTP response splitting/header injection;
- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors);
- Use of older, insecure SSL/TLS versions;
- Use of anonymous key exchange protocols (such as anonymous Diffie-Hellman in SSL/TLS); and
- Scan Interference.

77. The Nessus PCI scan also located three problems with Walmart.com's SSL/TLS certificates. SSL/TLS stands for Secure Sockets Layer/Transport Layer Security and is how websites encrypt data transmissions. SSL/TLS utilizes digital certificates to encrypt data. Security flaws in SSL/TLS certificates make all transmissions vulnerable, including transmissions of credit card information and account details.

78. The Nessus PCI scan identified the following problems with Walmart.com's SSL/TLS certificates: SSL certificate cannot be trusted, SSL certificate with wrong hostname, and SSL self-signed certificate. Each of these problems means that data transmissions on the website are vulnerable.

79. The Nessus PCI scan also revealed that Defendant is using an outdated protocol, TLS Version 1.1, which is technology that was replaced 12 years ago and has known weaknesses.

80. As a net result of these vulnerabilities in Walmart.com, it is possible for hackers to obtain large amounts of customer PII entered into and stored by Walmart.com in one fell swoop. Data stolen in such a manner would include customer PII that had been entered into Walmart.com prior to the date of the actual data breach itself. As such, the hacking of Walmart.com that occurred in 2020 would most likely also include data that was provided to Walmart in 2019 as well.

81. Under Walmart's duty to protect the PII, it was required to institute reasonable

1 security measures on its website to deter hacks. These vulnerabilities show that Walmart has
2 breached that duty.

3 82. Plaintiff and Class Members have suffered monetary injury in fact as a direct and
4 proximate result of the acts committed by Defendants, as alleged herein, in an amount to be
5 proven at trial, but in excess of the minimum jurisdictional amount of this Court.

6 83. Further, Plaintiff, Class Members, and future customers who make purchases
7 and/or open accounts on Walmart's website are at high risk of suffering, or have already suffered,
8 injuries that cannot be remedied monetarily, such as reductions to their credit scores and identity
9 theft. As such, the remedies at law available to Plaintiff and Class Members are wholly
10 inadequate by themselves. Injunctive relief – including mandating Defendants' compliance with
11 federal information security statutes and regulations – is both appropriate and necessary to prevent
12 further, irreparable harm to consumers resulting from the unabated harvesting of customer PII
13 from Walmart's website. The full extent of the existing and potential harm caused by Defendants'
14 failure to protect their customers' PII cannot be remedied by monetary damages alone because
15 monetary compensation does nothing to prevent the reoccurrence of another data breach in the
16 future.

17 **SECOND CAUSE OF ACTION**

18 (Negligence)

19 84. Plaintiff repeats and incorporates by reference each and every allegation contained
20 in paragraphs 1 through 83, inclusive of this Complaint as if set forth fully herein.

21 85. Defendants owed Plaintiff and the Class Members, as customers, a duty of care in
22 the handling of PII, which duty included keeping that PII safe and preventing disclosure of that
23 PII to all unauthorized third parties. This duty of care existed independently of Defendants'
24 contractual duty to Plaintiff and the Class Members. Under the CCPA, the Federal Trade
25 Commission ("FTC") Guidelines, and other sources of industry-wide standards, Defendants must
26 incorporate adequate measures to safeguard and protect the PII.

27 86. As noted, the CCPA creates a duty for all businesses in California to implement
28 and maintain reasonable security procedures and practices appropriate to the nature of the

1 information to protect personal information.

2 87. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
3 *Guide for Business*, which established guidelines for fundamental data security principles and
4 practices for business.⁴ Among other things, the guidelines note businesses should protect the
5 personal customer information that they keep; properly dispose of personal information that is no
6 longer needed; encrypt information stored on computer networks; understand their network's
7 vulnerabilities; and implement policies to correct security problems. The guidelines also
8 recommend that businesses use an intrusion detection system to expose a breach as soon as it
9 occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the
10 system; watch for large amounts of data being transmitted from the system; and have a response
11 plan ready in the event of a breach.⁵

12 88. Additionally, the FTC recommends that companies limit access to sensitive data;
13 require complex passwords to be used on networks; use industry-tested methods for security;
14 monitor for suspicious activity on the network; and verify that third-party service providers have
15 implemented reasonable security measures.⁶

16 89. The FTC has brought enforcement actions against businesses for failing to
17 adequately and reasonably protect customer information, treating the failure to employ reasonable
18 and appropriate measures to protect against unauthorized access to confidential consumer data as
19 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C.
20 § 45. Orders resulting from these actions further clarify the measures businesses must take to meet
21 their data security obligations.⁷

22 90. Additional industry guidelines which provide a standard of care can be found in
23

24 ⁴ Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct.
25 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last visited Nov. 22, 2019).

26 ⁵ *Id.*

27 ⁶ Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015)
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

28 ⁷ Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*
<https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement> (last visited Nov. 22, 2019).

the National Institute of Standards and Technology's ("NIST's") Framework for Improving Critical Infrastructure Cybersecurity, available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, attached hereto as **Exhibit H**. Among other guideposts, the NIST's framework identifies seven steps for establishing or improving a cybersecurity program (section 3.2). Those steps are:

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on

the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier. *Step 6: Determine, Analyze, and Prioritize Gaps.* The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

(Id.)

91. The PCI Data Security Standard ("DSS"), which includes a library of documents available at https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pci_dss_large_org, is also a source of duties of care applicable to Defendant. The PCI DSS sets forth specific security standards applicable to all businesses which process major credit cards, including Defendants. Included in the documents in the PCI DSS library is a document titled Best Practices for Maintaining PCI DSS Compliance, *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for

1 Maintaining_PCI_DSS_Compliance.pdf?agreement=true&time=1591897283857, attached
 2 hereto as **Exhibit I**. The entire document establishes a framework for obtaining and maintaining
 3 PCI DSS compliance, thereby establishing duties of care applicable to Defendant.

4 92. In addition to the PCI DSS library of compliance documents, there is the
 5 Requirements and Security Assessment itself: [https://www.pcisecuritystandards.org/documents/](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1591898978871)
 6 PCI_DSS_v3-2-1.pdf?agreement=true&time=1591898978871, attached hereto as **Exhibit J**,
 7 which sets forth specific requirements which a company must meet if it is to process major credit
 8 cards, as Defendants do. This document establishes numerous detailed duties which applies to
 9 Defendants, including requirement 6.5.7, which concerns cross-site scripting:

10 6.5.7: Examine software-development policies and procedures and interview
 11 responsible personnel to verify that XSS is addressed by coding techniques that
 12 include:

- 13 • Validating all parameters before inclusion;
- 14 • Utilizing context-sensitive escaping. (*Id.*) Other statutory duties can be
 15 found in California's Customer Records Act, Civ. Code §§ 1798.81.5
 16 (requiring reasonable data security measures) and 1798.82 (requiring timely
 17 breach notification).

18 93. In addition to Defendants' obligations under federal regulations and industry
 19 standards, Defendants owed a duty to Plaintiff and the Class Members to exercise reasonable care
 20 in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession
 21 from being compromised, lost, stolen, accessed, and misused by unauthorized persons.
 22 Defendants owed a duty to Plaintiff and the Class Members to provide reasonable security,
 23 including consistency with industry standards and requirements, and to ensure that their computer
 24 systems and networks, and the personnel responsible for them, adequately protected the PII of
 25 Plaintiff and the Class Members.

26 94. Defendants owed a duty to Plaintiff and the Class Members to design, maintain,
 27 and test their computer system to ensure that the PII in Defendants' possession was adequately
 28 secured and protected.

1 95. Defendants owed a duty to Plaintiff and the Class Members, to create and
2 implement reasonable data security practices and procedures to protect the PII in their possession,
3 including training their employees and others who accessed PII within their computer systems on
4 how to adequately protect PII.

5 96. Defendants owed a duty to Plaintiff and the Class Members to implement
6 processes that would detect a breach of their data security systems in a timely manner.

7 97. Defendants owed a duty to Plaintiff and the Class Members to act upon data
8 security warnings and alerts in a timely fashion.

9 98. Defendants owed a duty to Plaintiff and the Class Members to disclose whether
10 their computer systems and data security practices were inadequate to safeguard individuals' PII
11 from theft because such an inadequacy would be a material fact in their decision to entrust PII
12 with Defendants or to make credit card purchases from Defendants.

13 99. Defendants owed a duty to Plaintiff and the Class Members to disclose in a timely
14 and accurate manner when data breaches occurred.

15 100. Defendants owed a duty of care to Plaintiff and the Class Members because they
16 were foreseeable and probable victims of any inadequate data security practices. Defendants
17 collected PII from Plaintiff and the Class Members directly. Defendants knew that a breach of
18 its data systems would cause Plaintiff and the Class Members to incur damages.

19 101. Defendants breached their duties of care to safeguard and protect the PII which
20 Plaintiff and the Class Members entrusted to them. Defendants adopted inadequate safeguards to
21 protect the PII, and, as shown, failed to adopt industry-wide standards set forth above in their
22 supposed protection of the PII. Defendants failed to design, maintain, and test their computer
23 system to ensure that the PII was adequately secured and protected, failed to create and implement
24 reasonable data security practices and procedures, failed to implement processes that would detect
25 a breach of their data security systems in a timely manner, failed to disclose the breach in a timely
26 and accurate manner, and otherwise breached each of the above duties of care by implementing
27 lax security procedures which led directly to the breach.

28 102. Defendants breached the duties set forth in the CCPA, the FTC Guidelines,

California's Customer Records Act, Civ. Code §§ 1798.81.5, 1798.82, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and the PCI DSS. In violation of the CCPA, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. In violation of the FTC Guidelines, *inter alia*, Defendants did not protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identify and address security gaps. And, as shown, Defendant violated the PCI-DSS in at least the following ways, in addition to the other violations listed above:

- Vulnerabilities with a CVSS base score greater than or equal to 4.0;
- Unsupported operating systems;
- Internet reachable database servers;
- Presence of built-in or default accounts;
- Unrestricted DNS Zone transfers;
- Unvalidated parameters leading to SQL injection attacks;
- Cross-Site Scripting (XSS) flaws;
- Directory traversal vulnerabilities;
- HTTP response splitting/header injection;
- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors);
- Use of older, insecure SSL/TLS versions;
- Use of anonymous key exchange protocols (such as anonymous Diffie-Hellman in SSL/TLS); and
- Scan Interference.

103. Finally, in violation of the California Customer Records Act, Defendants failed to employ reasonable security measures, and failed to timely notify Plaintiff and the Class Members of the breach. Indeed, Defendants have, to date, failed to notify its customers of the breach.

104. As a direct and proximate result of Defendants’ failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft and theft of property, and for which Plaintiff and the Class members were forced to adopt costly and time-consuming preventive and remediating efforts. Plaintiff and the Class Members were also damaged in that they paid for goods sold by Defendants in an amount that they would have refused to pay had they known that Defendants would not protect their PII. These damages were magnified by the passage of time because Defendants failed to notify their customers of the data breach.

105. Plaintiff and Defendants were in a “special relationship” which eliminates the bar of recovery on economic harm for this claim. Under *J’Aire Corp. v. Gregory*, 24 Cal.3d 799, 804, 157 Cal.Rptr. 407, 410, 598 P.2d 60, 63 (1979), “[e]ven when only injury to prospective economic advantage is claimed, recovery is not foreclosed;” instead, “[w]here a special relationship exists between the parties, a plaintiff may recover for loss of expected economic advantage through the negligent performance of a contract.” *J’Aire* applies both where parties are in contractual privity and when they are not in contractual privity. *N. Am. Chem. Co. v. Superior Ct.*, 59 Cal. App. 4th 764, 783, 69 Cal. Rptr. 2d 466, 476 (1997) (citing *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal.App.4th 1439, 1448, 37 Cal.Rptr.2d 790 (1995)); *Pisano v. American Leasing*, 146 Cal.App.3d 194, 197, 194 Cal.Rptr. 77 (1983). “As the *Ott* court put it, ‘the reasoning of *J’Aire* is wholly incompatible with a limitation of the cause of action to those instances in which the plaintiff and defendant are not in privity, ...’” *N. Am. Chem. Co.*, 59 Cal. App. 4th at 783 (citing *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal.App.4th at 1448.)

106. Plaintiff satisfies each of the “special relationship” factors enumerated in *J’Aire*. “Those criteria are (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.” *J’Aire*, 24 Cal.3d at 804.

107. In *J'Aire*, “The contract entered into between respondent and the county was for the renovation of the premises in which appellant maintained its business.” *Id.* “The contract could not have been performed without impinging on that business.” *Id.* “Thus respondent's performance was intended to, and did, directly affect appellant.” *Id.* In short, the test for the first factor, the extent to which the transaction was intended to affect the plaintiff, was whether the contract could have been performed without affecting Plaintiff. Here, as Plaintiff engaged in the contract at issue, purchasing items from Defendants, the contract could not have been performed without affecting Plaintiff. Accordingly, the first factor is met.

108. As to the second factor, the foreseeability of harm to the Plaintiff, harm was most certainly foreseeable. In 2020, over 155.8 million Americans were affected by data exposures. <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-andrecordsexposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security/>. Hackers are constantly looking to invade business' systems and obtain the valuable PII of their customers. It is foreseeable that, if reasonable security measures are not taken, a business will be subject to a data breach, and its customers' data will be exposed to hackers. That is what happened.

109. As to the third factor, the degree of certainty that Plaintiff suffered injury, it is highly certain that Plaintiff did in fact suffer injury because his PII, including his credit card number and all data necessary to access the credit card account, was posted on the dark web for sale by hackers. Once this data is exposed on the dark web, it cannot be removed. Because Plaintiff's data was posted for sale on the dark web, it is virtually certain that his data will eventually be used by a hacker to commit fraud and identity theft unless Plaintiff goes to great lengths and expends money and time to protect himself.

110. As to the fourth factor, the closeness of the connection between Defendants' conduct and the injury suffered, there is a high degree of closeness of that connection, because Defendants' negligence in adopting adequate measures to protect the PII was a direct and proximate cause of the data breach. Due to the pervasive nature of hackers' attacks on businesses' systems, searching for customer PII, it was highly certain that hackers would attack Defendants'

1 systems and obtain data from them, given the vulnerabilities that those systems present. If a bank
2 does not lock its vault, and the money is stolen therefrom, there is a high degree of closeness
3 between the conduct of failing to lock the vault, and the theft. So too, here, where Defendants
4 failed to adequately protect their system from attack, there is a high degree of closeness between
5 that failure and the resultant theft of data.

6 111. As to the fifth factor, the moral blame attached to Defendants' conduct, there is a
7 high degree of moral blame because, in today's economy, consumers are forced to trust companies
8 with an internet presence to protect their data, which must be conveyed to companies in order to
9 transact business online. If we are to incentivize transactions over the internet, we must assess a
10 high level of moral blame to a company that does not protect its customers' PII because, without
11 that protection, consumers will stop transacting online, and the internet economy will die.

12 112. As to the fifth factor, the policy of preventing future harm, the only way to
13 incentivize companies like Walmart to protect consumers' PII is to hold them accountable when
14 their negligence in protecting that data results in a breach. To give force to the duties which,
15 through industry standards and regulations, exist as to the protection of data, there must be
16 consequences when those duties are breached. Otherwise those duties have no teeth, so to speak,
17 and they become mere words without consequences for lack of enforcement. In short, if we want
18 companies to protect their customers' data, and undertake the costly measures necessary to do so,
19 we must hold those companies liable when they do not protect that data. Companies like Walmart
20 can often evade damages for contract-related causes of action, leaving negligence as the only
21 means through which the courts can incentivize the important measures, central to our internet
22 economy, of protecting PII. If we want consumers to trust companies enough to transact business
23 online, and provide their PII over the internet, we must hold those companies responsible when
24 they breach that trust.

25 113. Plaintiff has suffered monetary injury in fact as a direct and proximate result of
26 the acts of negligence committed by Defendants as alleged herein in an amount to be proven at
27 trial but in excess of the minimum jurisdictional amount of this Court.
28

THIRD CAUSE OF ACTION

(Violation of the Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et. seq.*)

114. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 113, inclusive of this Complaint as if set forth fully herein.

115. By their actions and conduct as alleged herein, Defendants have committed one or more acts of unfair competition within the meaning of the UCL, Bus. & Prof. Code § 17200, that constitute unfair, unlawful and/or fraudulent business practices as those terms are defined under California law.

116. Defendants’ business practices are unfair under the UCL because Defendants have acted in a manner that is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to Plaintiff and the Class Members. The exposure of PII to third parties is substantially injurious because of the significant harm that can result to the customer at the hand of those third parties, and the protective measures that the customer must undertake as a direct result of this exposure. Further, the impact of the practice against Plaintiff and the Class Members far outweighs any possible justification or motive on the part of Defendants. Plaintiff and the Class Members could not reasonably have avoided this injury because they relied upon Defendants’ promises to protect and safeguard the PII from disclosure, as all consumers must who participate in today’s largely electronic market. Finally, Defendants have committed an unfair act by failing to notify its customers of the breach whatsoever.

117. Defendants’ failure to safeguard and protect Plaintiff’s and the Class Members’ PII is violative of public policy as expressed in the CCPA, the FTC publications, including, Protecting Personal Information: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last visited Nov. 22, 2019), the NIST’s Framework for Improving Critical Infrastructure Cybersecurity, and the PCI DSS. These regulations and guidelines set forth a clear public policy that companies such as Walmart take appropriate measures to prevent the exposure of customers’ PII to hackers, measures which, as shown *supra*, were not taken by Defendants here.

118. Defendants’ business practices are also unfair because they significantly threaten

1 or harm competition. Participation in today's credit economy is predicated on the security of the
2 PII of the participants in that economy, in the sense that PII is an asset of the individual which, if
3 lost to him or her, jeopardizes his or her very ability to maintain capital. Competitive economic
4 activity cannot exist where PII goes unprotected.

5 119. Defendants' business practices are unlawful under the UCL because Defendants
6 have violated the CCPA, the FTC Act, and California's Customer Records Act, Civ. Code §§
7 1798.81.5 and 1798.82. In violation of the CCPA, Defendants failed to implement and maintain
8 reasonable security procedures and practices appropriate to the nature of the information to
9 protect personal information. Defendants' conduct also constituted an unfair or deceptive practice
10 under the FTC Act because it "causes or is likely to cause substantial injury to consumers which
11 is not reasonably avoidable by consumers themselves and not outweighed by countervailing
12 benefits to consumers or to competition." 15 U.S.C. 45(n). Consumers cannot avoid the injury
13 themselves because they are not informed of the severe vulnerabilities presented by the website.
14 There is no benefit to consumers or competition to a vulnerable website, so the injury cannot be
15 outweighed by any such countervailing benefit. In violation of the Customer Records Act,
16 Defendants failed to institute reasonable security measures, and failed to notify Plaintiff and the
17 Class Members of the breach whatsoever.

18 120. Plaintiff has suffered monetary injury in fact as a direct and proximate result of
19 the acts of unfair competition committed by Defendants, as alleged herein, in an amount to be
20 proven at trial, but in excess of the minimum jurisdictional amount of this Court. Plaintiff suffered
21 a monetary injury when he was forced to purchase credit monitoring services and undertake other
22 efforts to reduce the risk of identity theft from the security breach. These are direct pecuniary
23 losses which are attributable to Defendants' violation of the UCL.

24 121. Plaintiff also suffered a monetary injury because he did not receive the benefit of
25 his bargain with Defendants, through which he agreed to pay for goods with the understanding
26 that his payment information would be protected by Defendants. Plaintiff would not have paid
27 the price he agreed to pay for the goods if he had known that Defendants would not protect his
28 PII.

122. Plaintiff also suffered a monetary injury when he lost the value of his PII, which is an exclusive asset of each individual with intrinsic and calculable monetary value. Now that his PII has been exposed to hackers and sold on the dark web, Plaintiff has wrongfully been deprived of the fair market value of his PII.

FOURTH CAUSE OF ACTION

(Breach of Express Contract)

123. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 122, inclusive of this Complaint as if set forth fully herein.

124. Defendants entered into an express contract with Plaintiff and the Class Members, pursuant to which they provided Defendants with their PII, and Defendants sold them goods. This contract incorporated Walmart's Privacy Policy, which Walmart posts on its website at <https://corporate.walmart.com/privacy-security/walmart-privacy-policy>, and which is attached hereto as **Exhibit K**. The privacy policy promises that Walmart will only share the PII with specified persons and entities, none of which are the hackers who obtained the PII in this case.

125. Plaintiffs and the Class Members performed everything that they were required to do under the contract by supplying their PII and paying for the goods in question. All conditions required for Defendants' performance have occurred or were excused.

126. The Privacy Policy states, "We will not share your personal information outside of our corporate family of companies, except in the following circumstances," and proceeds to list eight categories of recipients, none of which were the hackers in this case. (*Id.* at p. 5-6)

127. Further, the Privacy Policy promises that Defendants will adopt reasonable security measures to protect the data in its possession, stating:

How Do We Secure Your Personal Information?

We recognize the importance of maintaining the security of our customers' personal information. ***We use reasonable security measures, including physical, administrative, and technical safeguards to protect your personal information.***

We have a team of associates who are responsible for helping to protect the security of your information. ***Whether you are shopping on our websites, through***

1 *our mobile services, or in our stores, we use reasonable security measures,*
2 *including physical, administrative, and technical safeguards.* These measures
3 may include physical and technical security access controls or other safeguards,
4 information security technologies and policies, procedures to help ensure the
5 appropriate disposal of information, and training programs.

6 (*Id.* at p. 9). (emphasis added).

7 128. Defendants breached these promises. As shown, Defendants allowed hackers to
8 obtain the PII, and did not limit its dissemination to the parties set forth in the Privacy Policy.
9 Defendant also failed to adopt reasonable security measures to protect the data, as illustrated by
10 the innumerable security vulnerabilities its website exhibits.

11 129. As a result of these breaches, Plaintiff and the Class Members were damaged.
12 Plaintiff and the Class Members' PII is being sold by nefarious individuals on the dark web. As
13 a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit
14 monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. Plaintiff and
15 the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members
16 agreed to purchase goods and provide their PII to Defendants with the understanding that their
17 PII would be protected. Had Plaintiff and the Class Members known that their PII would not be
18 protected, they would not have agreed to pay the price which they contracted for in exchange for
19 the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen,
20 that they will lose money, and that their identities will be stolen as a result of the breach. That
21 risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members
22 have lost the value of their PII, which has a real market value.

23 130. Plaintiff and the Class Members' losses were caused by Defendants' breach. By
24 allowing the hackers to obtain the PII, Defendants caused Plaintiff and the Class Members to
25 incur out-of-pocket expenses, lose the benefit of their bargain, incur the risk of identity and
26 property theft, and lose the value of their PII. By failing to institute reasonable measures to protect
27 the data, each of these categories of damages were also caused, because the hackers breached
28 Defendants' system and Plaintiff's and the Class Members' computers and accounts due to the

1 vulnerabilities on the website.

2 131. To the extent that Defendants plan to raise the limitation of liability and disclaimer
3 of warranty clauses as a bar to Plaintiff's contract-based causes of action, those clauses are
4 substantively and procedurally unconscionable, and cannot be enforced.

5 132. First, as to procedural unconscionability, the contract at issue is an adhesion
6 contract, and is therefore afforded a substantial level of procedural unconscionability. Second,
7 when Plaintiff entered the contract, it contained terms that purported to state promises as to which
8 Defendants would be bound. It was procedurally unconscionable to take those promises away in
9 subsequent clauses, which might not even be found by a consumer reading the contract for the
10 first time, which clauses eliminated the mutuality of the contract, as Defendants would not be
11 bound under them for any promises whatsoever. By presenting an agreement, and making
12 promises therein, Defendants indicated that there were terms under the agreement as to which
13 both parties would be bound. Taking those promises away amounts to an unfair surprise, which
14 is procedurally unconscionable. Moreover, the contradictory clauses created confusion on the
15 part of the Plaintiff, as it is unclear which provision controls—the provision making the promise,
16 or the provision taking it away.

17 133. Second, as to substantive unconscionability, the clauses are substantively
18 unconscionable because they eliminate the mutuality of the agreement, rendering it a unilateral
19 document which imposes requirements on the consumer, but imposes no obligation or restriction
20 on Defendants. Lack of mutuality is the height of substantive unconscionability. Moreover, it
21 accords with public policy to interpret contracts so as to render them enforceable. If the clauses
22 are interpreted as Defendants suggest, the agreement cannot be enforced, because it is utterly
23 lacking in mutual consideration. If the clauses are enforced, then no contract was formed, and
24 Plaintiff should be permitted to proceed on a quasi-contract, or unjust enrichment theory.

25 134. Plaintiff has suffered monetary injury in fact as a direct and proximate result of
26 the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in
27 excess of the minimum jurisdictional amount of this Court.
28

FIFTH CAUSE OF ACTION

(Breach of Implied Contract)

135. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 134, inclusive of this Complaint as if set forth fully herein.

136. Defendants and Plaintiff and the Class Members entered an implied contract governing the use and protection of PII when Plaintiff and the Class Members supplied their PII in order to purchase goods from Defendants. Plaintiffs and the Class Members performed everything that they were required to do under the contract by supplying their PII and paying for the goods in question. All conditions required for Defendants' performance have occurred or were excused.

137. This contract was manifested in the conduct of the parties. By agreeing to take Plaintiff's and the Class Members' PII into its possession, Defendants impliedly agreed to protect that PII from hackers, who were known to attempt to steal PII by hacking entities which possess it, to adopt reasonable measures to protect the PII from hackers, and to timely notify Plaintiff and the Class Members of a data breach should one occur. Defendants knew, or had reason to know, that by taking the PII, they were engaging in conduct that would lead Plaintiff and the Class Members to believe that Defendants would protect that data from exposure to hackers, due to the known risk of hacking, which was understood by both parties to the contract. Other conduct which gives rise to this contractual agreement is Defendants' adoption of passwords through which Plaintiff and the Class Members ostensibly kept their information private, the posting of a Privacy Policy, and tips to protect personal data, on Defendants' website.

138. Defendants breached these promises. As shown, Defendants allowed hackers to obtain the PII. Defendants also failed to adopt reasonable security measures to protect the data, as illustrated by the innumerable security vulnerabilities its website exhibits. Finally, Defendants failed to notify its customers of the data breach whatsoever.

139. As a result of these breaches, Plaintiff and the Class Members were damaged. Plaintiff's and the Class Members' PII is being sold by nefarious individuals on the dark web. As a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit

1 monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. Plaintiff and
 2 the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members
 3 agreed to purchase goods and provide their PII to Defendants with the understanding that their
 4 PII would be protected. Had Plaintiff and the Class Members known that their PII would not be
 5 protected, they would not have agreed to pay the price which they contracted for in exchange for
 6 the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen,
 7 that they will lose money, and that their identities will be stolen as a result of the breach. That
 8 risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members
 9 have lost the value of their PII, which has a real market value.

10 140. Plaintiff's and the Class Members' losses were caused by Defendants' breach. By
 11 allowing the hackers to obtain the PII, Defendant caused Plaintiff and the Class Members to incur
 12 out-of-pocket expenses, lose the benefit of their bargain, incur the risk of identity and property
 13 theft, and lose the value of their PII. By failing to institute reasonable measures to protect the
 14 data, each of these categories of damages were also caused, because the hackers breached
 15 Defendants' system and Plaintiff's and the Class Members' computers and accounts due to the
 16 vulnerabilities on the website.

17 141. Plaintiff has suffered monetary injury in fact as a direct and proximate result of
 18 the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in
 19 excess of the minimum jurisdictional amount of this Court.

20 **SIXTH CAUSE OF ACTION**

21 (Breach of the Implied Covenant of Good Faith and Fair Dealing)

22 142. Plaintiff repeats and incorporates by reference each and every allegation contained
 23 in paragraphs 1 through 141, inclusive of this Complaint as if set forth fully herein.

24 143. Plaintiff and the Class Members entered contracts with Defendants for the sale of
 25 goods, which incorporated the Privacy Policy, and which also included the implied terms that
 26 Defendant would not expose the PII to hackers and that Defendants would take reasonable
 27 measures to protect the PII.

28 144. In these contracts, as in every contract, there was an implied covenant of good

1 faith and fair dealing. This implied promise means that each party will not do anything to unfairly
2 interfere with the right of any other party to receive the benefits of the contract. Good faith means
3 honesty of purpose without any intention to mislead or to take unfair advantage of another, that
4 is, being faithful to one's duty or obligation.

5 145. Plaintiffs and the Class Members performed everything that they were required to
6 do under the contract by supplying their PII and paying for the goods in question. All conditions
7 for Defendants' performance have occurred or were excused.

8 146. Defendants failed to protect the PII from exposure to hackers, and failed to adopt
9 reasonable measures to protect the PII, operating a website with numerous security flaws as
10 shown above. Defendants also failed to notify Plaintiff and the Class Members of the breach, so
11 that they could make reasonable efforts to protect their identities and property.

12 147. By doing so, Defendants did not act fairly and in good faith. Good faith and
13 fairness required Defendants to protect the PII from hackers, including by adopting reasonable
14 measures. Consumers must count on companies who collect their PII to protect that PII in order
15 to facilitate commercial transactions, which increasingly occur over the internet.

16 148. As a result of this conduct, Plaintiff and the Class Members were damaged.
17 Plaintiff's and the Class Members' PII is being sold by nefarious individuals on the dark web. As
18 a result, Plaintiff and the Class Members have been forced to incur out of pocket costs for credit
19 monitoring, and to take time and effort to cancel credit cards and/or freeze accounts. Plaintiff and
20 the Class Members have also lost the benefit of their bargain. Plaintiff and the Class Members
21 agreed to purchase goods and provide their PII to Defendants with the understanding that their
22 PII would be protected. Had Plaintiff and the Class Members known that their PII would not be
23 protected, they would not have agreed to pay the price which they contracted for in exchange for
24 the goods. Plaintiff and the Class Members also face a significant risk that their PII will be stolen,
25 that they will lose money, and that their identities will be stolen as a result of the breach. That
26 risk only increases as time passes and no action is taken. Finally, Plaintiff and the Class Members
27 have lost the value of their PII, which has a real market value.

28 149. Plaintiff has suffered monetary injury in fact as a direct and proximate result of

the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

SEVENTH CAUSE OF ACTION

(Unjust Enrichment)

150. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 149, inclusive of this Complaint as if set forth fully herein.

151. When Plaintiff transacted with Defendants over the internet for the purchase of goods, Defendants received a benefit from Plaintiff in the form of the price of the item purchased. Plaintiff believed that some portion of this price would be used to pay for measures to protect his PII from disclosure to unauthorized individuals.

152. Defendants did not pay for the cost of maintaining and/or increasing security measures on its website such that Plaintiff's and Class Members' PII would not be stolen. Instead, Defendants retained this benefit as profit, and left Plaintiff's and Class Members' PII exposed on its website for hackers to access. As a result, hackers accessed the data and posted it for sale on the dark web.

153. Accordingly, Defendants received a benefit from Plaintiff and Class Members and retained that benefit, rather than using it to protect their customers at their customers' expense.

154. Plaintiff is entitled to either: (1) restitution of the full price he paid for the goods, or (2) restitution of that portion of the price which would be used to provide data protection for Plaintiff's PII.

155. Plaintiff has suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants, as alleged herein, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for relief as follows:

1. For compensatory damages in an amount according to proof at trial;
2. For affirmative injunctive relief mandating that Defendants implement and

maintain reasonable security procedures and practices to protect Plaintiff's and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure, and notify Plaintiff and the Class Members of all data breaches which have occurred;

3. For costs of suit and litigation expenses;

4. For attorneys' fees under the common fund doctrine and all other applicable law; and


5. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: March 26, 2021

Respectfully submitted,



Thiago M. Coelho
Justin F. Marquez
Robert J. Dart
April Yang
WILSHIRE LAW FIRM, PLC

*Attorneys for Plaintiff
and the Proposed Class*